A MOD-p ARTIN-TATE CONJECTURE, AND GENERALIZED HERBRAND-RIBET

DIPENDRA PRASAD

March 11, 2018

Abstract. Following the natural instinct that when a group operates on a number field then every term in the class number formula should factorize 'compatibly' according to the representation theory (both complex and modular) of the group, we are led — in the spirit of Herbrand-Ribet's theorem on the p-component of the class number of $\mathbb{Q}(\zeta_p)$ — to some natural questions about the p-part of the classgroup of any CM Galois extension of $\mathbb{Q}$ as a module for $\mathrm{Gal}(K/\mathbb{Q})$. The compatible factorization of the class number formula is at the basis of *Stark's conjecture*, where one is mostly interested in factorizing the regulator term — whereas for us in this paper, we put ourselves in a situation where the regulator term can be ignored, and it is the factorization of the classnumber that we seek. All this is presumably part of various 'equivariant' conjectures in arithmetic-geometry, such as 'equivariant Tamagawa number conjecture', but the literature does not seem to address this question in any precise way. In trying to formulate these questions, we are naturally led to consider $L(0,\rho)$, for ρ an Artin representation, in situations where this is known to be nonzero and algebraic, and it is important for us to understand if this is $\mathfrak{p}$-integral for a prime $\mathfrak{p}$ of the ring of algebraic integers $\bar{\mathbb{Z}}$ in $\mathbb{C}$, that we call *mod-p Artin-Tate conjecture*. As an attentive reader will notice, the most minor term in the class number formula, the number of roots of unity, plays an important role for us — it being the only term in the denominator, is responsible for all the poles!

Contents

1. Introduction

Let F be a number field contained in $\mathbb{C}$ with $\bar{\mathbb{Q}}$ its algebraic closure in $\mathbb{C}$. Let $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_n(\mathbb{C})$ be an irreducible Galois representation with $L(s,\rho)$ its associated Artin L-function. According to a famous conjecture of Artin, $L(s,\rho)$ has an analytic continuation to an entire function on $\mathbb{C}$ unless ρ is the trivial representation, in which case it has a unique pole at $s = 1$ which is simple.

More generally, let M be an irreducible motive over $\mathbb{Q}$ with $L(s,M)$ its associated L-function. According to Tate, $L(s,M)$ has an analytic continuation to an entire function on $\mathbb{C}$ unless M is a twisted Tate motive $\mathbb{Q}[j]$ with $\mathbb{Q}[1]$ the motive associated to $\mathbb{G}_m$.

For the motive $\mathbb{Q} = \mathbb{Q}[0]$, $L(s, \mathbb{Q}) = \zeta_{\mathbb{Q}}(s)$, the usual Riemann zeta function, which has a unique pole at $s = 1$ which is simple.

This paper will deal with certain Artin representations $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_n(\mathbb{C})$ for which we will know a priori that $L(0, \rho)$ is a nonzero algebraic number (in particular, F will be totally real). It is then an important question to understand the nature of the algebraic number $L(0, \rho)$: to know if it is an algebraic integer, but if not, what are its possible denominators. We think of the possible denominators in $L(0, \rho)$, as existence of poles for $L(0, \rho)$, at the corresponding prime ideals of $\bar{\mathbb{Z}}$. It is thus analogous to the conjectures of Artin and Tate, both in its aim — and as we will see — in its formulation. Since we have chosen to understand L-values at 0 instead of 1 which is where Artin and Tate conjectures are formulated, there is an 'ugly' twist by ω_p — the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the p-th roots of unity — throughout the paper, giving a natural character $\omega_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p)^\times$, also a character of $\mathrm{Gal}(\bar{\mathbb{Q}}/L)$ for L any algebraic extension of $\mathbb{Q}$, as well as a character of $\mathrm{Gal}(L/\mathbb{Q})$ if L is a Galois extension of $\mathbb{Q}$ containing p-th roots of unity; if there are no non-trivial p-th roots of unity in L, we will define ω_p to be the trivial character of $\mathrm{Gal}(L/\mathbb{Q})$.

We now fix some notation. We will fix an isomorphism of $\bar{\mathbb{Q}}_p$ with $\mathbb{C}$ where $\bar{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$, the field of p-adic numbers. This allows one to define $\mathfrak{p}$, a prime ideal in $\bar{\mathbb{Z}}$, the integral closure of $\mathbb{Z}$ in $\mathbb{C}$, over the prime ideal generated by p in $\mathbb{Z}$. The prime p will always be an odd prime in this paper.

All the finite dimensional representations of finite groups in this paper will take values in $\mathrm{GL}_n(\bar{\mathbb{Q}}_p)$, and therefore in $\mathrm{GL}_n(\mathbb{C})$, as well as $\mathrm{GL}_n(\bar{\mathbb{Z}}_p)$. It thus makes sense to talk of 'reduction modulo $\mathfrak{p}$' of (complex) representations of finite groups. These reduced representations are well defined up to semi-simplification on vector spaces over $\bar{\mathbb{F}}_p$ (theorem of Brauer-Nesbitt); we denote the reduction modulo $\mathfrak{p}$ of representations as $\rho \to \bar{\rho}$.

If F is a finite Galois extension of $\mathbb{Q}$ with Galois group G, then it is well-known that the zeta function $\zeta_F(s)$ can be factorized as

$$\zeta_F(s) = \prod_{\rho} L(s, \rho)^{\dim \rho},$$

where ρ ranges over all the irreducible complex representations of G, and $L(s, \rho)$ denotes the Artin L-function associated to ρ.

According to the class number formula, we have,

$$\zeta_F(s) = -\frac{hR}{w} s^{r_1 + r_2 - 1} + \text{ higher order terms},$$

where r_1, r_2, h, R, w are the standard invariants associated to F: r_1, the number of real embeddings; r_2, number of pairs of complex conjugate embeddings which are not real; h, the class number of F; R, the regulator, and w the number of roots of unity in F.

This paper considers ζ_E/ζ_F where E is a CM field with F its totally real subfield, in which case $r_1 + r_2$ is the same for E as for F, and the regulators of E and F too are the same except for a possible power of 2. Therefore for τ the complex conjugation on $\mathbb{C}$,

$$\zeta_E/\zeta_F(0) = \prod_{\rho(\tau) = -1} L(0, \rho)^{\dim \rho} = \frac{h_E/h_F}{w_E/w_F},$$

where each of the L-values $L(0,\rho)$ in the above expression are nonzero algebraic numbers by a theorem of Siegel.

In this identity, observe that L-functions are associated to $\mathbb{C}$-representations of $\mathrm{Gal}(E/\mathbb{Q})$, whereas the classgroups of E and F are finite Galois modules. Modulo some details, we basically assert that for each odd prime p, each irreducible $\mathbb{C}$-representation ρ of $\mathrm{Gal}(E/\mathbb{Q})$ contributes a certain number of copies (depending on $\mathfrak{p}$-adic valuation of $L(0,\rho)$) of $\bar{\rho}$ to the classgroup of E tensored with $\mathbb{F}_p$ modulo the classgroup of F tensored with $\mathbb{F}_p$ (up to semi-simplification). This is exactly what happens for $E = \mathbb{Q}(\zeta_p)$ by the theorems of Herbrand and Ribet which is one of the main motivating example for all that we do here, and this is what we will review next.

2. The Herbrand-Ribet theorem

In this section we recall the Herbrand-Ribet theorem from the point of view of this paper. We refer to [Ri1] for the original work of Ribet, and [Was] for an exposition on the theorem together with a proof of Herbrand's theorem.

There are actually two a priori important aspects of the Herbrand-Ribet theorem dealing with the p-component of the classgroup for $\mathbb{Q}(\zeta_p)$. First, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p)^\times$, being a cyclic group of order $(p-1)$, its action on the p-component of the classgroup is semi-simple, and the p-component of the classgroup can be written as a direct sum of eigenspaces for $(\mathbb{Z}/p)^\times$. We do not consider this aspect of Herbrand-Ribet theorem to be important, and simply consider semi-simplification of representations of Galois group on classgroups to be a good enough substitute.

The second — and more serious — aspect of Herbrand-Ribet theorem is that among the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p)^\times$, only the odd characters, i.e., characters $\chi : (\mathbb{Z}/p)^\times \to \mathbb{Q}_p^\times$ with $\chi(-1) = -1$ present themselves — as it is only for these that there is any result about the χ-eigencomponent in the classgroup, and even among these, the Teichmüller character $\omega_p : (\mathbb{Z}/p)^\times \to \mathbb{Q}_p^\times$ plays a role different from other characters of $(\mathbb{Z}/p)^\times$. (Note that earlier we have used ω_p for the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the p-th roots of unity, giving a natural character $\omega_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p)^\times$, as well as to its restriction to $\mathrm{Gal}(\bar{\mathbb{Q}}/L)$ for L any algebraic extension of $\mathbb{Q}$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/p)^\times$, the two roles that ω_p will play throughout the paper are actually the same.)

To elaborate on this aspect (the role of 'odd' characters in Herbrand-Ribet theorem), observe that the class number formula

$$\zeta_F(s) = -\frac{hR}{w} s^{r_1+r_2-1} + \text{ higher order terms},$$

can be considered both for $F = \mathbb{Q}(\zeta_p)$ as well as its maximal real subfield $F^+ = \mathbb{Q}(\zeta_p)^+$. It is known that, cf. Prop 4.16 in [Was],

$$R/R^+ = 2^{\frac{p-3}{2}},$$

where R is the regulator for $\mathbb{Q}(\zeta_p)$ and R^+ is the regulator for $\mathbb{Q}(\zeta_p)^+$. We will similarly denote h and h^+ to be the order of the two class groups, with $h^- = h/h^+$, an integer.

Dividing the class number formula of $\mathbb{Q}(\zeta_p)$ by that of $\mathbb{Q}(\zeta_p)^+$, we find,

$$\prod_{\chi \text{ an odd character of } (\mathbb{Z}/p)^\times} L(0,\chi) = \frac{1}{p} \cdot \frac{h}{h^+} \cdot 2^{\frac{p-3}{2}}, \qquad (*)$$

the factor $1/p$ arising because there are $2p$ roots of unity in $\mathbb{Q}(\zeta_p)$ and only 2 in $\mathbb{Q}(\zeta_p)^+$.

It is known that for χ an odd character of $(\mathbb{Z}/p)^\times$, $L(0,\chi)$ is an algebraic number which is given in terms of the generalized Bernoulli number $B_{1,\chi}$ as follows:

$$L(0,\chi) = -B_{1,\chi} = -\frac{1}{p}\sum_{a=1}^{a=p} a\chi(a).$$

It is easy to see that $pB_{1,\omega_p^{p-2}} \equiv (p-1) \bmod p$ since $a\omega_p^{p-2}(a)$ is the trivial character of $(\mathbb{Z}/p)^\times$ whereas for all the other characters of $(\mathbb{Z}/p)^\times$, $L(0,\chi)$ is not only an algebraic number but is p-adic integral (Schur orthogonality!); all this is clear by looking at the expression:

$$L(0,\chi) = -B_{1,\chi} = -\frac{1}{p}\sum_{a=1}^{a=p} a\chi(a).$$

Rewrite the equation $(*)$ up to p-adic units as,

$$\prod_{\substack{\chi \text{ an odd character of } (\mathbb{Z}/p)^\times \\ \chi \neq \omega_p^{p-2} = \omega_p^{-1}}} L(0,\chi) = \frac{h}{h^+},$$

where we note that both sides of the equality are p-adic integral elements; in fact, since all characters $\chi : (\mathbb{Z}/p)^\times \to \bar{\mathbb{Q}}_p^\times$ take values in $\mathbb{Z}_p$, for $\chi \neq \omega_p^{-1}$, $L(0,\chi) \in \mathbb{Z}_p$. This when interpreted — just an interpretation in the optic of this paper without any suggestions for proof in either direction! — for each χ component on the two sides of this equality amounts to the theorem of Herbrand and Ribet which asserts that p divides $L(0,\chi) = -B_{1,\chi}$ for χ an odd character of $(\mathbb{Z}/p)^\times$, which is not ω_p^{p-2}, if and only if the corresponding χ^{-1}-eigencomponent of the classgroup of $\mathbb{Q}(\zeta_p)$ is nontrivial. (Note the χ^{-1}, and not χ!) Furthermore, the character ω_p does not appear in the p-classgroup of $\mathbb{Q}(\zeta_p)$. It can happen that $L(0,\chi)$ is divisible by higher powers of p than 1, and one expects — this is not proven yet! — that in such cases, the corresponding χ^{-1}-eigencomponent of the classgroup of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}/p^{(\mathrm{val}_p L(0,\chi))}$, in particular, it still has p-rank 1. (By Mazur-Wiles [Ma-Wi], χ^{-1}-eigencomponent of the classgroup of $\mathbb{Q}(\zeta_p)$ is of order $p^{(\mathrm{val}_p L(0,\chi))}$.)

The work of Ribet was to prove that if $p|B_{1,\chi}$, χ^{-1}-eigencomponent of the classgroup of $\mathbb{Q}(\zeta_p)$ is nontrivial by constructing an unramified extension of $\mathbb{Q}(\zeta_p)$ by using a congruence between a holomorphic cusp form and an Eisenstein series on $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.

To be able to use the class number formula in other situations, we will need to have the integrality of $L(0,\chi)$ for χ a character associated to the Galois group of a number field, or even of $L(0,\rho)$ for general irreducible representations ρ of the Galois group

of a number field, in more situations that we call mod p Artin-Tate conjecture. We begin with the following lemma.

Lemma 1. *Let ℓ, p be any two odd primes ($\ell = p$ is allowed). Let F be a totally real number field, and $E = F(\zeta_{p^n})$ be a quadratic CM extension of F. Let $h_\ell^-(E)$ be the order of the ℓ-primary part of the classgroup of E on which complex conjugation acts by -1; define $h_\ell^-(\mathbb{Q}(\zeta_{p^n}))$ similarly. Then*

$$h_\ell^-(\mathbb{Q}(\zeta_{p^n}))|h_\ell^-(E).$$

Proof. By classfield theory, it suffices to prove that a cyclic degree ℓ unramified extension, say L, of $\mathbb{Q}(\zeta_{p^n})$ on which complex conjugation acts by -1 on $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{p^n})) \cong \mathbb{Z}/\ell$ when inflated to E remains cyclic of degree ℓ, i.e., the degree of LE/E is ℓ. Assuming the contrary, we have $LE = E$, and since degree of E/F is 2, and p is odd, we must have $LF = F$, i.e., $L \subset F$, therefore complex conjugation must act trivially on L. On the other hand, we know that complex conjugation does not act trivially on L. □

Remark 1. It may be noted that we are not asserting that if $\mathbb{Q}(\zeta_{p^n}) \subset E, h(\mathbb{Q}(\zeta_{p^n}))|h(E)$.

Let E be a CM number field which we assume is Galois over $\mathbb{Q}$. Assume that E contains p^n-th roots of unity but no p^{n+1}-st root of unity. Let F be the totally real subfield of E with $[E : F] = 2$. Let $G = \mathrm{Gal}(E/Q)$ with $-1 \in G$, the complex conjugation in G.

We have,

$$\zeta_E(s) = \prod_\rho L_{\mathbb{Q}}(s,\rho)^{\dim\rho},$$

$$\zeta_F(s) = \prod_{\rho(-1)=1} L_{\mathbb{Q}}(s,\rho)^{\dim\rho},$$

$$\zeta_E/\zeta_F(s) = \prod_{\rho(-1)=-1} L_{\mathbb{Q}}(s,\rho)^{\dim\rho},$$

where all the products above are over irreducible representations ρ of $G = \mathrm{Gal}(E/\mathbb{Q})$.

By the class number formula,

$$h^-(E)/p^n = \prod_{\rho(-1)=-1} L_{\mathbb{Q}}(0,\rho)^{\dim\rho} \quad (\star 1).$$

Similarly,

$$h^-(\mathbb{Q}(\zeta_{p^n}))/p^n = \prod_{\chi(-1)=-1} L_{\mathbb{Q}}(0,\chi) \quad (\star 2).$$

Dividing the equation $(\star 1)$ by $(\star 2)$, we have,

$$h^-(E)/h^-(\mathbb{Q}(\zeta_{p^n})) = \prod_{\substack{\rho(-1)=-1,\\ \rho\neq\chi}} L_{\mathbb{Q}}(0,\rho)^{\dim\rho} \quad (\star 3),$$

where the product on the right is taken over irreducible representations ρ of $G = \mathrm{Gal}(E/\mathbb{Q})$ for which $\rho(-1) = -1$, and which are not cyclotomic characters of the form $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n)^\times \to \mathbb{C}^\times$.

It is known that $L(0,\rho) \in \bar{\mathbb{Q}}^\times$ for $\rho(-1) = -1$. This is a simple consequence of Siegel's theorem that partial zeta functions of a totally real number field take rational

values at all non-positive integers, cf. Tate's book [Tate]. (Note that to prove $L(0,\rho) \in \bar{\mathbb{Q}}^\times$ for $\rho(-1) = -1$, it suffices by Brauer to prove it for abelian CM extensions by a Lemma of Serre cf. Lemma 1.3 of Chapter III of Tate's book [Tate].)

By Lemma 1, the left hand side of the equation $(\star 3)$ is integral (except for powers of 2), and we would like to suggest the same for each term on the right hand side of the equation $(\star 3)$.

The following conjecture about $L(0,\rho)$ extends the known integrality properties of $L(0,\chi) = -B_{1,\chi} = -\frac{1}{p}\sum_{a=1}^{a=p} a\chi(a)$, encountered and used earlier. The formulation of the conjecture also assumes known integrality properties about $L(0,\chi)$ for $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$ discussed in the last section of this paper.

Conjecture 1. *(mod p analogue of the Artin-Tate conjecture) Let ρ be an irreducible representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ cutting out a CM extension E of $\mathbb{Q}$ with $\rho(-1) = -1$ where -1 is the complex conjugation in $\mathrm{Gal}(E/\mathbb{Q})$. Then unless ρ is one dimensional representation factoring through $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ (for some prime p) with $\bar{\rho}$ the reduction of ρ modulo p being $\bar{\rho} = \omega_p^{-1}$, $L(0,\rho) \in \bar{\mathbb{Q}}$ is integral outside 2, i.e., $L(0,\rho) \in \bar{\mathbb{Z}}[\frac{1}{2}]$.*

We next recall the following theorem of Deligne-Ribet, cf. [DR], which could be considered as a weaker version of Conjecture 1.

Theorem. *Let F be a totally real number field, and let $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \bar{\mathbb{Q}}^\times$ be a character of finite order cutting out a CM extension K of F (which is not totally real). Let w be the order of the group of roots of unity in K. Then,*

$$wL(0,\chi) \in \bar{\mathbb{Z}}.$$

In fact Conjecture 1 can be used to make precise the above theorem of Deligne-Ribet as follows; the simple argument using the fact that the Artin L-function is invariant under induction from $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ will be left to the reader.

Conjecture 2. *Let F be a totally real number field, and $\chi : \mathbb{A}_F^\times/F^\times \to \bar{\mathbb{Z}}_p^\times$ a finite order character, cutting out a non-real but CM extension. Then if $L_F(s,\chi) \notin \bar{\mathbb{Z}}_p$,*

(1) χ mod p is ω_p^{-1}.
(2) χ is a character of $\mathbb{A}_F^\times/F^\times$ associated to a character of the Galois group $\mathrm{Gal}(F(\zeta_q)/F)$ for some q which is a power of p.

Remark 2. In the examples that I know, which are for characters $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}_p^\times$ with $\chi = \omega_p^{-1} \pmod p$, if $L(0,\chi)$ has a (mod p) pole, the pole is of order 1; more precisely, if $L = \mathbb{Q}_p[\chi(\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p))]$ is the subfield of $\bar{\mathbb{Q}}_p$ generated by the image under χ of the decomposition group at p, then $L(0,\chi)$ is the inverse of a uniformizer of this field L. It would be nice to know if this is the case for characters χ of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ for F arbitrary. This would be in the spirit of classical Artin's conjecture where the only possible poles of $L(1,\rho)$, for ρ an irreducible representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$, are simple.

Conjecture 3. *Let F be a totally real number field, and let $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ be a semi-simple modular representation of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ cutting out a finite CM extension E of F with E not totally real. Assume that $\omega_p \otimes \bar{\rho}$ does not contain the trivial*

representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ *where* ω_p *is the action of* $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ *on the* p*-th roots of unity. Then it is possible to define* $\bar{L}(0,\bar{\rho}) \in \bar{\mathbb{F}}_p$ *with*

$$\bar{L}(0,\bar{\rho}_1+\bar{\rho}_2) = \bar{L}(0,\bar{\rho}_1)\cdot\bar{L}(0,\bar{\rho}_2),$$

for any two such representations $\bar{\rho}_1$ *and* $\bar{\rho}_2$*, and such that, if* $\bar{\rho}$ *arises as the semi-simplification of reduction mod-*p *of a representation* $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ *cutting out a finite CM extension* E *of* F *with* E *not totally real, then* $L(0,\rho)$ *which belongs to* $\bar{\mathbb{Z}}_p$ *by Conjecture 1 has its reduction mod-*p *to be* $\bar{L}(0,\bar{\rho})$*.*

The conjecture above requires that if two representations $\rho_1, \rho_2 : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ have the same semi-simplification mod-p and do not contain the character ω_p^{-1}, then $L(0,\rho_1)$ and $L(0,\rho_2)$ (which are in $\bar{\mathbb{Z}}_p$ by Conjecture 1) have the same reduction mod-p. By a well-known theorem of Brauer, a modular representation $\bar{\rho}$ can be lifted to a virtual representation $\sum n_i\rho_i$ in characteristic 0. However, since $L(0,\rho_i)$ may be zero mod-p, for some i (for which $n_i < 0$), the theorem of Brauer does not guarantee that $L(0,\bar{\rho})$ can be defined.

3. Proposed generalization of Herbrand-Ribet for CM number fields

The Herbrand-Ribet theorem is about the relationship of L values $L(0,\chi)$ with the χ^{-1}-eigencomponent of the classgroup of $\mathbb{Q}(\zeta_p)$. In the last section, we have proposed a precise conjecture about integrality properties for the L values $L(0,\rho)$. In this section, we now propose their relationship to classgroups.

Let E be a Galois CM extension of $\mathbb{Q}$ with F the totally real subfield of E with $[E:F] = 2$. Let G denote the Galois group of E over $\mathbb{Q}$. Let τ denote the element of order 2 in the Galois group of E over F. As in the last section,

$$\zeta_E/\zeta_F(0) = \prod_{\rho(\tau)=-1} L(0,\rho)^{\dim\rho} = \frac{h_E}{h_F}\frac{1}{w_E},$$

where the product is taken over all irreducible representations ρ of $G = \mathrm{Gal}(E/\mathbb{Q})$ with $\rho(\tau) = -1$, and w_E denotes the group of roots of unity of E considered as a module for G.

Let H_E (resp. H_F) denote the class group of E (resp. F). Observe that the kernel of the natural map from H_F to H_E is a 2-group. (This follows from using the norm mapping from H_E to H_F.) Therefore since we are interested in p-primary components for only odd primes p, H_F can be considered to be a subgroup of H_E, and the quotient H_E/H_F becomes a G-module of order h_E/h_F.

Conjecture 4. *Let* E *be a CM, Galois extension of* $\mathbb{Q}$ *with* F *its totally real subfield, and* $\tau \in \mathrm{Gal}(E/F)$*, the nontrivial element of the Galois group. Let* $\rho : \mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ *be an irreducible, odd (i.e.,* $\rho(\tau) = -1$*) representation of* $\mathrm{Gal}(E/\mathbb{Q})$ *with* $\bar{\rho}$ *its reduction mod* $\mathfrak{p}$ *for* p *an odd prime. Let* $\omega_p : \mathrm{Gal}(E/\mathbb{Q}) \to (\mathbb{Z}/p)^\times$ *be the action of* $\mathrm{Gal}(E/\mathbb{Q})$ *on the* p*-th roots of unity in* E *(so* $\omega_p = 1$ *if* $\zeta_p \notin E$*). Write* $\bar{\rho} = \sum n_i\bar{\rho}_i$*, and let* $\bar{\rho}_j$ *be a component in this sum. Then if* $\bar{\rho}_j \neq \omega_p^{-1}$*, and* $\bar{L}(0,\bar{\rho}_j) = 0 \in \bar{\mathbb{F}}_p$ *(cf. Conjecture 2)* $[H_E/H_F]\otimes\bar{\mathbb{F}}_p$ *contains* $n_j\dim(\rho)\bar{\rho}_j^\vee$ *in its semi-simplification, with different* ρ*'s contributing independently to the semi-simplification of* $[H_E/H_F]\otimes\bar{\mathbb{F}}_p$*, filling it up except for the* ω_p*-component. If* $\omega_p \neq 1$*,*

we make no assertion on the ω_p-component in $[H_E/H_F] \otimes \bar{\mathbb{F}}_p$, but if $\omega_p = 1$, there is no ω_p-component inside $[H_E/H_F] \otimes \bar{\mathbb{F}}_p$ (see remark 3 below).

Remark 3. In the context of this conjecture, there is a question in representation theory which plays a role too: Given a finite group G, what are the finite dimensional irreducible representations $\rho : G \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ such that the mod-p representation $\bar{\rho}$ contains the trivial representation of G in its semi-simplification? See the lemma below.

In our context with CM fields etc., there is one case which does not involve dealing with this subtle question. To elaborate on this, let G be a finite group together with a character $\omega_p : G \to (\mathbb{Z}/p)^\times$, and with a central element τ of order 2, i.e., $\tau^2 = 1$; the question is to understand the finite dimensional irreducible representations $\rho : G \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ such that the mod-p representation $\bar{\rho}$ contains the character ω_p of G in its semi-simplification with $\rho(\tau) = -1$? If the character $\omega_p \neq 1$, then we further are given that $\omega_p(\tau) = -1$. However, $\omega_p : G \to (\mathbb{Z}/p)^\times$ might be the trivial character corresponding to the CM field E having no p-th roots of unity. In this case, there are no such irreducible representations $\rho : G \to \mathrm{GL}_n(\bar{\mathbb{Q}}_p)$ such that the mod-p representation $\bar{\rho}$ contains the character $\omega_p^{-1} = 1$, because $\rho(\tau) = -1$ continues to hold mod-p!

Lemma 2. *Let G be a finite group, and p a prime number dividing the order of G. Then the number of trivial representations of G appearing in the semi-simplification of $\mathbb{F}_p[G]$ equals $|P| \cdot a_p(G)$, where P is a p-Sylow subgroup of G, and $a_p(G) \geq 1$ denotes the number of trivial representations of G appearing in the semi-simplification of $\mathbb{F}_p[G/P]$. In particular, there are always non-trivial irreducible $\mathbb{C}$-representations of G whose reduction mod-p contains the trivial representation of G.*

Proof. Observe that

$$\mathbb{F}_p[G] = \mathrm{Ind}_P^G \mathrm{Ind}_{\{e\}}^P \mathbb{F}_p = \mathrm{Ind}_P^G(\mathbb{F}_p[P]).$$

Since any irreducible representation of P (in characteristic p) is the trivial representation, the semi-simplification of $\mathbb{F}_p[P]$ is the same as $|P|$ copies of the trivial representation. Conclusion of the lemma follows. □

Remark 4. The integer $a_p(G) \geq 1$ introduced in this lemma seems of interest. For $G = \mathrm{PGL}_2(\mathbb{F}_p)$, $a_p(G) = 1$. For any group G in which a p-Sylow subgroup is normal, or more generally in a group G with a p-Sylow subgroup P, and another subgroup H of G of order coprime to p with $G = HP$, we have $a_p(G) = 1$. The author is grateful to Bhama Srinivasan for conveying an example of Paul Fong that for $p = 5$, and $G = A_5$, the number $a_5(A_5) = 2$.

Remark 5. I should add that Ribet's theorem is specific to $\mathbb{Q}(\zeta_p)$ and although this section is very general, it could also be specialized to a CM abelian extension E of $\mathbb{Q}$, and the action of the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ on the full class group of E. Since class group of an abelian extension is not totally obvious from the classgroup of the corresponding cyclotomic field $\mathbb{Q}(\zeta_n)$, even if we knew everything in the style of Ribet for $\mathbb{Q}(\zeta_n)$, presumably there is still some work left to be done, and not just book keeping (for n which is a composite number)!

4. Integrality of Abelian L-values for $\mathbb{Q}$

The aim of this section is to prove certain results on integrality of $L(0,\chi)$ for χ an odd Dirichlet character of $\mathbb{Q}$ which go as first examples of all the integrality conjectures made in this paper. Although these are all well-known results, we have decided to give our proofs.

Lemma 3. *For integers $m > 1, n > 1$, with $(m,n) = 1$, let $\chi = \chi_1 \times \chi_2$ be a primitive Dirichlet character on $(\mathbb{Z}/mn\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ with $\chi(-1) = -1$. Then,*

$$L(0,\chi) = -B_{1,\chi} = -\frac{1}{mn}\sum_{a=1}^{mn} a\chi(a),$$

is an algebraic integer, i.e., belongs to $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$.

Proof. Observe that $B_{1,\chi} = \frac{1}{mn}\sum_{a=1}^{mn} a\chi(a)$, has a possible fraction by mn, and that in this sum over $a \in \{1,2,\cdots,mn\}$, if we instead sum over an arbitrary set A of integers which have these residues mod mn, then $\frac{1}{mn}\sum_{a\in A} a\chi(a)$, will differ from $B_{1,\chi}$ by an integral element (in $\bar{\mathbb{Z}}$). Since our aim is to prove that $B_{1,\chi}$ is integral, it suffices to prove that $\frac{1}{mn}\sum_{a\in A} a\chi(a)$ is integral for some set of representatives $A \subset \mathbb{Z}$ of residues mod mn.

For an integer $a \in \{1,2,\cdots,m\}$, let $\bar{a}$ be an arbitrary integer whose reduction mod m is a, and whose reduction mod n is 1. Similarly, for an integer $b \in \{1,2,\cdots,n\}$, let $\bar{b}$ be an arbitrary integer whose reduction mod n is b and whose reduction mod m is 1. Clearly, the set of integers $\bar{a}\cdot\bar{b}$ represents — exactly once — each residue class mod mn, and that $\bar{a}\cdot\bar{b}$ as an element in $\mathbb{Z}$ goes to the pair $(a,b) \in \mathbb{Z}/m \times \mathbb{Z}/n$. (It is important to note that $\bar{a}\cdot\bar{b}$ as an element in $\mathbb{Z}$ is *not* congruent to ab mod mn, and therein lies a subtlety in the Chinese remainder theorem: there is no simple inverse to the natural isomorphism: $\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$.)

By definition of the character χ, $\chi(\bar{a}\cdot\bar{b}) = \chi_1(a)\chi_2(b)$. It follows that,

$$\frac{1}{mn}\sum \bar{a}\bar{b}\chi(\bar{a}\cdot\bar{b}) - \left[\frac{1}{m}\sum_{a=1}^{m} a\chi_1(a)\right]\cdot\left[\frac{1}{n}\sum_{b=1}^{n} b\chi_2(b)\right] \in \bar{\mathbb{Z}}. \qquad (\star)$$

Since the character χ is odd, one of the characters, say χ_2 is even (and χ_1 is odd).

Observe that,

$$B_{1,\chi_2} = \frac{1}{n}\sum_{b=1}^{n} b\chi_2(b) = \frac{1}{n}\sum_{b=1}^{n}(n-b)\chi_2(b).$$

It follows that,

$$\frac{2}{n}\sum_{b=1}^{n} b\chi_2(b) = \sum_{b=1}^{n}\chi_2(b) = 0,$$

where the last sum is zero because the character χ_2 is assumed to be non-trivial.

Since

$$\frac{1}{mn}\sum \bar{a}\bar{b}\chi(\bar{a}\cdot\bar{b}) - \frac{1}{mn}\sum_{c=1}^{mn} c\chi(c) \in \bar{\mathbb{Z}},$$

by the equation $(\star)$, it follows that:

$$\frac{1}{mn}\sum_{c=1}^{mn} c\chi(c) \in \bar{\mathbb{Z}},$$

as desired. □

Lemma 4. *For p a prime, let χ be a primitive Dirichlet character on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ with $\chi(-1) = -1$. Write $(\mathbb{Z}/p^n\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}/1+p^n\mathbb{Z})$, and the character χ as $\chi_1 \times \chi_2$ with respect to this decomposition. Then,*

$$L(0,\chi) = -B_{1,\chi} = -\frac{1}{p^n}\sum_{a=1}^{p^n} a\chi(a),$$

is an algebraic integer, i.e., belongs to $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$ if and only if $\chi_1 \neq \omega_p^{-1}$.

Proof. Assuming that $\chi_1 \neq \omega_p^{-1}$, we prove that $B_{1,\chi}$ belongs to $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$.

By an argument similar to the one used in the previous lemma, it can be checked that,

$$\frac{1}{p^n}\sum_{a=1}^{p^n} a\chi(a) - \left[\frac{1}{p}\sum_{a=1}^{p} a\chi_1(a)\right] \cdot \left[\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}} (1+bp)\chi_2(1+bp)\right] \in \bar{\mathbb{Z}}. \qquad (\star).$$

If $\chi_1 \neq \omega_p^{-1}$, $\frac{1}{p}\sum_{a=1}^{p} a\chi_1(a)$ is easily seen to be integral. To prove the lemma, it then suffices to prove that, $\left[\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}} (1+bp)\chi_2(1+bp)\right]$ is integral.

Note the isomorphism of the additive group $\mathbb{Z}_p$ with the multiplicative group $1+p\mathbb{Z}_p$ by the map $n \to (1+p)^n \in 1+p\mathbb{Z}_p$. Let $\chi_2(1+p) = \alpha$ with $\alpha^{p^{n-1}} = 1$.

Then (the first and third equality below is up to $\bar{\mathbb{Z}}$),

$$\begin{aligned}
\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}} (1+bp)\chi_2(1+bp) &= \frac{1}{p^{n-1}}\sum_{c=1}^{p^{n-1}} (1+p)^c\alpha^c \\
&= \frac{1}{p^{n-1}}\sum_{c=1}^{p^{n-1}} [\alpha(1+p)]^c \\
&= \frac{1}{p^{n-1}}\frac{1-[\alpha(1+p)]^{p^{n-1}}}{1-\alpha(1+p)} \\
&= \frac{1}{p^{n-1}}\frac{[1-(1+p)^{p^{n-1}}]}{[1-\alpha(1+p)]}.
\end{aligned}$$

Note that since $\alpha^{p^{n-1}} = 1$ either $\alpha = 1$, or $1-\alpha$ is a uniformizer in $\mathbb{Q}_p(\zeta_{p^d})$ for some $d \leq n-1$. Therefore either $-p = [1-\alpha(1+p)]$ if $\alpha = 1$, or $[1-\alpha(1+p)]$ is a uniformizer in $\mathbb{Q}_p(\zeta_{p^d})$. Finally, it suffices to observe that,

$$(1+p)^{p^{n-1}} \equiv 1 \bmod p^n,$$

hence, $\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}} (1+bp)\chi_2(1+bp)$ is integral.

If $\chi_1 = \omega_p^{-1}$, the same argument gives non-integrality; we omit the details. □

The following proposition follows by putting the previous two lemmas together, and making an argument similar to what went into the proof of these two lemmas. We omit the details.

Proposition 1. *Primitive Dirichlet characters $\chi : (\mathbb{Z}/n)^\times \to \bar{\mathbb{Z}}_p^\times$ for which $L(0,\chi)$ does not belong to $\bar{\mathbb{Z}}_p$ are exactly those for which:*

(1) $n = p^d$.
(2) $\chi = \omega_p^{-1}$ mod $\mathfrak{p}$.

The following consequence of the proposition suggests that prudence is to be exercised when discussing congruences of L-values for Artin representations which are congruent. (Our formulation of Conjecture 3 excludes the characters which are involved in the corollary below.)

Corollary 1. *Let p, q be odd primes with $p|(q-1)$. For any character χ_2 of $(\mathbb{Z}/q\mathbb{Z})^\times$ of order p, define the character $\chi = \omega_p^{-1} \times \chi_2$ of $(\mathbb{Z}/pq\mathbb{Z})^\times$. Then although the characters ω_p^{-1} and χ have the same reduction modulo p, $L(0,\omega_p^{-1})$ is p-adically non-integral whereas $L(0,\chi)$ is integral.*

Question 1. Let $\chi : (\mathbb{Z}/p^d m)^\times \to \bar{\mathbb{Z}}_p^\times$ with $(p,m) = 1$, $m > 1$, be a primitive Dirichlet character for which $\chi = \omega_p^{-1}$ mod $\mathfrak{p}$ so that by Proposition 1, $L(0,\chi)$ is $\mathfrak{p}$-integral. Is it possible to have $L(0,\chi) = 0$ modulo $\mathfrak{p}$, the maximal ideal of $\bar{\mathbb{Z}}_p$? Our proofs in this section are 'up to $\bar{\mathbb{Z}}$', so good to detect integrality, but not good for questions modulo $\mathfrak{p}$. The question is relevant to conjecture 4 to see if the character ω_p appears in the classgroup H/H^+ for $E = \mathbb{Q}(\zeta_{p^d m})$; such a character is known not to appear in the classgroup of H/H^+ for $E = \mathbb{Q}(\zeta_{p^d})$.

Acknowledgement: The author thanks P. Colmez for suggesting that the questions posed here are not as outrageous as one might think, and for even suggesting that some of the conjectures above should have an affirmative answer as a consequence of the Main conjecture of Iwasawa theory for totally real number fields proved by A. Wiles [Wiles] if one knew the vanishing of the μ-invariant (which is a conjecture of Iwasawa proved for abelian extensions of $\mathbb{Q}$ by Ferrero-Washington). The author also thanks U.K. Anandavardhanan, C. Dalawat, C. Khare for their comments and their encouragement.

References

[DR] P. Deligne, K. Ribet, *Values of abelian L-functions at negative integers over totally real fields,* Invent. Math. 59 (1980), no. 3, 227–286.

[Lang] S. Lang, Cyclotomic fields I and II. Combined second edition. With an appendix by Karl Rubin. Graduate Texts in Mathematics, 121. Springer-Verlag, New York, 1990.

[Ma-Wi] B. Mazur, A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$. Invent. Math. 76 (1984), no. 2, 179–330.

[Ri1] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$*, Invent. Math.,* 34, 151-162 (1976).

[Tate] J. Tate, Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$, *Birkhauser, Progress in mathematics, vol. 47* (1984).

[Was] L. C. Washington, Introduction to Cyclotomic Fields, *GTM, Springer-Verlag, vol. 83*, (1982).

[Wiles] A. Wiles, *The Iwasawa conjecture for totally real fields.* Ann. of Math. (2) 131 (1990), no. 3, 493–540.

Dipendra Prasad

Tata Insititute of Fundamental Research, Colaba, Mumbai-400005, INDIA.
e-mail: dprasad@math.tifr.res.in